AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated below.

1. (Currently Amended) In a personal computer having encryption hardware and a processor, a method of storing data on one or more magnetic or optical data storage media in an encrypted form comprising:

storing an identification code in a non-erasable memory during manufacture of the personal computer, wherein said identification code is defined at least in part by information associated with components of said personal computer;

retrieving the identification code from the non-erasable memory in said personal computer;

receiving user input;

generating a cryptographic key derived at least in part from said identification code and the received user input;

retrieving a checksum from a configuration register in a bus-to-bus bridge in the personal computer, the bus-to-bus bridge storing information identifying which of the one or more magnetic or optical data storage media is selected to receive encrypted data;

verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated cryptographic key;

retrieving information from a memory location;

disabling encryption of data routed to one of the one or more magnetic or optical data storage media in response to said retrieved information;

encrypting and decrypting data based on the disabling step, for storage on and retrieval from one of ~~said~~the one or more magnetic or optical data storage media using the ~~said~~the generated cryptographic key, wherein the data is transmitted by the processor and is encrypted in the personal computer by the encryption hardware; and

~~retrieving information from a memory location; and~~

~~disabling encryption of data routed to one of media in response to said retrieved information.~~

storing the data in the one or more magnetic or optical data storage media either in encrypted form or non-encrypted form based on the disabling step.

2. (Canceled)

3. (Currently Amended) The method of Claim 1, wherein said retrieving the identification code is performed without intervention by a host processor.

4. (Currently Amended) The method of Claim 3, ~~additionally comprising verifying said key,~~ wherein said verifying occurs without intervention of said host processor.

5. (Currently Amended) A method of making a computer comprising:

storing a hardware identifier in a non-erasable memory integrated circuit at the time of manufacture of ~~the~~said computer, wherein the hardware identifier is defined at least in part by information associated with components of said computer~~, the bus-to-bus bridge storing information identifying which data storage media is selected to receive encrypted data~~;

installing said non-erasable memory integrated circuit into said computer;

providing a data path to the data storage media;

providing a configuration register in a bus-to-bus bridge for storing a checksum, the bus-to-bus bridge storing information identifying which data storage media is selected to receive encrypted data;

coupling a logic circuit comprising an encryption engine to said data path; and

connecting said non-erasable memory integrated circuit to said logic circuit, wherein the hardware identifier and a user input is used by the encrypting engine for encrypting data that is transmitted to the data storage media and for decrypting data that is retrieved from the data storage media, wherein the encryption engine verifies the generated cryptographic key using the checksum, and wherein the encryption engine is configured to disable encryption of data routed to the data storage media in response to information retrieved from a storage location.

6. (Currently Amended) The method of Claim 5, wherein said act of connecting comprises routing a serial data bus from said non-erasable memory integrated circuit to said logic circuit.

7. (Currently Amended) In a computer system comprising a processor and encryption hardware and at least one data storage device, a method of data storage comprising:

receiving user input;

transmitting data from the processor in the computer system to the encryption hardware in the computer system; and

generating a cryptographic key derived at least in part from the received user input and information that is stored in a non-erasable memory in said computer system during manufacture of said computer system;

retrieving a checksum from a configuration register in a bus-to-bus bridge in ~~the~~said computer system, the bus-to-bus bridge register storing information identifying which storage device is selected to receive encrypted data;

verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated key;

retrieving information from a memory location;

disabling encryption of data routed to said selected data storage device in response to said retrieved information;

encrypting and decrypting, in the encryption hardware, user generated data with an encryption process that uses the generated cryptographic key, the encrypting and decrypting being based on the disabling step;

~~retrieving information from a memory location; and~~

~~disabling encryption of data routed to said data storage device in response to said retrieved information.~~

storing the data in the at least one storage device either in encrypted form or non-encrypted form based on the disabling step.

8. (Previously Presented) The method of Claim 7, wherein said information is permanently associated with said host computing logic.

9. (Previously Presented) The method of Claim 7, wherein said information comprises a multi-bit identification code.

10. (Currently Amended) The method of Claim 9, additionally comprising the act of deriving an encryption key at least in part from said multi-bit identification code.

11. (Canceled)

12. (Previously Presented) The method of Claim 7, additionally comprising defining said encryption process at least in part from user input to said computer system.

13. (Currently Amended) The method of Claim 1, wherein encrypting data for storage is performed on an encrypting device that is positioned in a data path between a central processing unit and ~~the data storage medium~~one of the one or more magnetic or optical data storage media.

14. (Currently Amended) The method of Claim 1, wherein all data that is transmitted to the one or more magnetic or optical ~~data storage~~ data storage media is encrypted.

15. (Currently Amended) In a personal computer having encryption hardware and a processor, a method of storing data on one or more magnetic or optical data storage media in an encrypted form comprising:

storing an identification code in a non-erasable memory during manufacture of the personal computer, wherein said identification code is defined at least in part by information associated with components of said personal computer;

retrieving the identification code from the non-erasable memory in said personal computer;

receiving user input;

generating a cryptographic key derived at least in part from said identification code and the received user input;

retrieving a checksum from a configuration register in a bus-to-bus bridge circuit in ~~the~~said personal computer, the bus-to-bus bridge circuit storing information identifying which of said one or more magnetic or optical storage media is selected to receive encrypted data;

verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated key;

retrieving information from a memory location;

disabling encryption of data routed to one of said storage media in response to said retrieved information;

encrypting and decrypting data based on the disabling step, for storage on and retrieval from one of said one or more magnetic or optical data storage media using said cryptographic key, wherein the data is transmitted by the processor and is encrypted in the personal computer by the encryption hardware, and wherein the encryption hardware is part of the bus-to-bus bridge circuit; and

~~retrieving information from a memory location; and~~

~~disabling encryption of data routed to one of said storage media in response to said retrieved information.~~

storing the data in one or more magnetic or optical data storage media in either encrypted form or non-encrypted form based on the disabling step.

16. (Canceled)

17. (Currently Amended) The method of Claim 15, wherein said retrieving the identification code is performed without intervention by a host processor.

18. (Currently Amended) The method of Claim 17, ~~additionally comprising verifying said key,~~ wherein said verifying occurs without intervention of said host processor.